

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

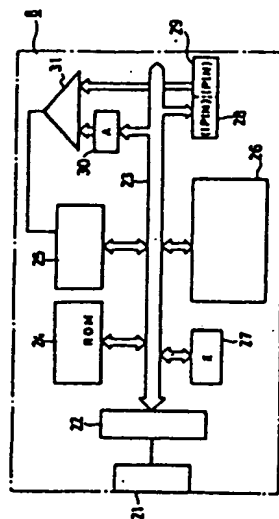
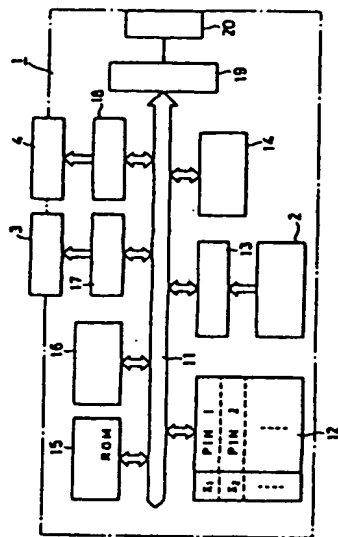
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

(54) CONFIRMING DEVICE FOR PASSWORD INFORMATION OF INTEGRATED
CIRCUIT CARD

- (11) 62-9471 (A) (43) 17.1.1987 (19) JP
(21) Appl. No. 60-147782 (22) 5.7.1985
(71) CASIO COMPUT CO LTD (72) HIDEO SUZUKI
(51) Int. Cl. G06F15/30, G07F7/08

PURPOSE: To confirm again a password number even in case the owner of an integrated circuit IC card forgets his/her password number, by having comparison between the password information stored previously in accordance with a specified IC card and the password number stored by said IC card itself.

CONSTITUTION: An end of an IC card 8 is put into the card slit of a printer electronic calculator 1 containing a terminal to secure the electrical connection between connection terminals 20 and 21. Then the data X proper to the card 8 is extracted through an IC card specifying data memory 27 and transmitted in the form of the card specifying data. At the terminal side the corresponding proper data X_1 is retrieved out of a password information memory 12 based on the specifying data X_1 . Then the stored password number is recognized and specified as a number corresponding to the card 8. Then this specified password number is extracted out of the memory 12 and sent to the card 8 to be held by an password information holding RAM 30. Then a comparing part 31 compares the password number stored in the RAM 30 with that stored in the memory 29.



2: keyboard, 3: display part, 4: print part, 13: input control part, 14: arithmetic control part, 15, 24: system ROM, 16, 25: system control part, 17: display control part, 18: print control part, 19, 22: interface part, 26: bankbook memory

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭62-9471

⑬ Int.Cl.⁴

G 06 F 15/30
G 07 F 7/08

識別記号

庁内整理番号

8219-5B
B-7234-3E

⑭ 公開 昭和62年(1987)1月17日

審査請求 未請求 発明の数 1 (全8頁)

⑮ 発明の名称 ICカード用暗証情報確認装置

⑯ 特 願 昭60-147782

⑰ 出 願 昭60(1985)7月5日

⑱ 発 明 者 鈴木 秀 夫 東京都西多摩郡羽村町栄町3丁目2番1号 カシオ計算機株式会社羽村技術センター内

⑲ 出 願 人 カシオ計算機株式会社 東京都新宿区西新宿2丁目6番1号

明 細 書

1. 発明の名称

ICカード用暗証情報確認装置

2. 特許請求の範囲

予めICカードの暗証情報を記憶するICカード用暗証情報確認装置において、接続されるICカード固有の番号を入力しそのカードの種類を認識する手段と、このカード認識手段により特定されたICカードに対応する上記予め記憶した暗証情報と上記特定ICカード自身の記憶する暗証情報とを比較照合する手段と、この照合手段により上記互いの暗証情報が一致したことを判定した際にその暗証情報を出力する手段とを具備したことを特徴とするICカード用暗証情報確認装置。

3. 発明の詳細な説明

〔発明の技術分野〕

この発明は、例えば銀行等の金融機関が発行するキャッシュカードあるいはクレジットカードとして使用されるICカードの暗証情報を必要に応じて出力するICカード用暗証情報確認装置に関

する。

〔従来技術とその問題点〕

近年はキャッシュレス時代と呼ばれており、クレジットカード会社等により発行されたカードを使用することにより、現金の取扱いをせずに商品の購入が可能となっている。上記カードとしては、従来、プラスチックカード、エンボスカード、磁気ストライプカード等が一般に使用されているが、これらのカードは構造上偽造が簡単であり、不正使用が問題になっている。このような問題を解決するため、最近ではカード内に、暗証番号等を記憶したIC回路を組み込み、暗証番号が外部から容易に読出せないようにした情報カード、所謂ICカードが開発されている。このICカードは偽造が困難で秘密性に優れ、また、多数の情報を記憶できるという利点があるばかりか、特に、個人の暗証番号を本人によって直接設定入力することができるため、本人以外の何人(例えば銀行員)にも暗証番号が知れることがなく、非常に安全性の高いものである。

しかしながら上記のようなICカードを使用するにあたっては、カード所有者本人が自分の暗証番号を忘れてしまうことが往々にしてあり、暗証番号を全く他人に知られないこのICカードにあつては、上記カード所有者本人が暗証番号を思い出さない限りカードを廃棄するしかないという問題がある。

〔発明の目的〕

この発明は上記のような問題点に鑑みなされたもので、例えばカード所有者本人が自分の暗証番号を忘れてしまった場合でも、カード内部に記憶された暗証情報を再び確認することができるようになるICカード用暗証情報確認装置を提供することを目的とする。

〔発明の要点〕

すなわちこの発明に係わるICカード用暗証情報確認装置は、ICカードに対する暗証情報の読み込みと同時に予め本装置にもその暗証情報を記憶させておき、後に接続されるICカードからの固有番号によりそのカードの種類を認識し、この認

識された特定ICカードに対応して上記予め記憶させた暗証情報を出力確認できるように構成したものである。

〔発明の実施例〕

以下図面によりこの発明の一実施例を説明する。

第1図はそのICカード用暗証情報確認装置の外観構成を示すもので、本装置のターミナル付プリンタ電卓1には、その本体上面にキーボード2、表示部3およびプリンタ4が設けられている。上記キーボード2は、テンキー、ファンクションキー等の演算用キーと共に、IPINキー5およびPINキー6を備えている。上記IPINキー5は、本体側部に設けられたカード挿入口7に接続されるICカード8に対して、照合番号IPIN(Initialization Personal Identification Number)を入力する際に使用され、また、PINキー6は、同様にして暗証番号PIN(Personal Identification Number)を登録する際に使用される。上記照合番

号IPINは、ランダムな例えば6ビットのコードで、カード所有者の暗証番号PINが使用されるまでのコードである。また、上記カード挿入口7の設けられる本体部同一側面には、切換スイッチ9を設け、暗証情報確認時におけるICカード8からの入力データの種別を選択する。

次に、第2図により上記ターミナル付プリンタ電卓1の回路構成について説明する。

図面において11はバスラインで、このバスライン11には、複数のICカードの暗証情報を記憶する暗証情報メモリ12、キーボード2を制御する入力制御部13、演算制御部14、システムROM15、システム制御部16、表示部3を制御する表示制御部17、プリンタ(印字部)4を制御する印字制御部18が接続される。また、上記バスライン11には、インターフェイス部19より接続端子20を介してICカード8が接続される。上記暗証情報メモリ12は、接続端子20により接続されるICカード8に対して、キーボード2よりバスライン11およびインターフェイ

ス部19を介して暗証情報を登録する際に、この登録と同時にそのICカード固有のデータが書込まれたメモリ位置に対応して上記暗証情報を予め記憶するもので、ここでは、複数種のICカードそれぞれの固有データX₁、X₂、…に対応する暗証情報をPIN1、PIN2、…として示している。ここで、上記カード固有のデータX₁、X₂、…は本ターミナルによりICカード8のPINの設定登録を行なった際に、該ICカード8より読出され設定されるデータである。この暗証情報メモリ12に記憶された各カード特定の暗証情報PIN1、PIN2、…は、接続されるICカード8からの後述するOK信号を受けて取出され、表示制御部17を介して表示部3に、あるいは印字制御部18を介して印字部4に出力される。

次に、第3図によりICカード8の回路構成について説明する。

図面において、21は上記第2図におけるプリンタ電卓1の接続端子20に相対する接続端子であり、接続端子21はインターフェイス部22を

介してバスライン23に接続される。そして、このバスライン23には、システムROM24、システム制御部25、通帳メモリ26およびICカード特定化データメモリ27が接続される。このICカード特定化データメモリ27には、個々のICカードを識別するための各カード毎に異なる、例えば64ビットのデータXが記憶されるもので、このカード固有のデータXはカード製造時において例えばカード会社固有のデータとして書込まれる。また、上記通帳メモリ26には、入金、出金、残高等の諸データが書込まれる。さらに、上記バスライン23には、IPINメモリ28、PINメモリ29および暗証情報保持用RAM30が接続される。上記IPINメモリ28には、予めカード製造時において書込まれた照合番号(IPIN)が、PINメモリ29には、このカード8を上記ターミナル付プリンタ電卓1に接続した際に、カード所有者本人にてキーボード2より書込まれる暗証番号(PIN)が記憶される。一方、上記暗証情報保持用RAM30には、上記プリンタ電

卓1のキーボード2より入力される照合番号IPINが、あるいは搬送するある一定の条件に基づいて暗証情報メモリ12より取出された暗証番号PINが、それぞれインターフェイス部19、22を介して供給され一時記憶保持される。そして、このIPINメモリ28およびPINメモリ29と暗証情報保持用RAM30とには比較部31が接続され、この比較部31からの比較出力信号は上記システム制御部25に供給される。この比較部31は、上記各メモリ28、29にて記憶された照合番号(IPIN)あるいは暗証番号(PIN)と、上記RAM30により一時記憶保持される照合番号IPINあるいは暗証番号PINとを比較照合し、そのそれぞれが互いに一致しているか否かを判定するもので、一致の場合システム制御部25はOKメッセージをプリンタ電卓1に送出し、一致しない場合にはBADメッセージを送出する。

次に、カード発行会社よりカード使用者に送られてくるICカード8及び別便にて送られてくる

照合番号IPINの情報に基づいて上記実施例装置にて上記ICカード8に暗証番号PINを設定する場合の動作を、第4図および第5図に示すフローチャートを参照して説明する。

第4図はターミナル付プリンタ電卓1内のフローチャートを、第5図はICカード8内のフローチャートを示すもので、まず始めに、ステップA1において、ターミナル付プリンタ電卓1のカード挿入口7に対してICカード8の一端を挿入し、ターミナル側の接続端子20とカード側の接続端子21との電気的接続を図る。次にステップA2に進み、上記ICカード8とは別便にてカード会社より送られてくる照合番号IPINをキーボード2にて入力する。そしてステップA3にて、上記IPINデータをインターフェイス部19および接続端子20を介してICカード8側へ送る。するとICカード8側では、ステップB1において、上記ターミナル側より送られて来た照合番号IPINデータを受信し、暗証情報保持用RAM30に一時記憶保持する。この後ステップB2に

進み、この照合番号IPINと予めIPINメモリ28にて記憶された照合番号(IPIN)とを比較部31にて比較照合し、そのそれぞれが一致しているか否かを判定する。このステップB2にてY(Yes)、つまり上記互いの照合番号は一致しており[IPIN=(IPIN)]、このICカード8を所有する人物が正規なカード所有者であると判定されると、ステップB3に進み、カード側のシステム制御部25はインターフェイス部22を介してOKメッセージを送信する。するとターミナル側では、ステップA4にて上記カード側からのメッセージ信号を受信し、ステップA5にてそのメッセージ信号がOKメッセージであるか否かを判定する。このステップA5にてY(Yes)と判定されると、ステップA6に進み、カード所有者はキーボード2を使用して自分自身が任意に設定した暗証番号PINを入力する。この後ステップA7に進み、上記の如く入力した暗証番号PINをカード側に送信すると共に、ステップA8にて上記ICカード8から読出される特

定化データX及び上記暗証番号PINが暗証情報メモリ12に記憶される。これに伴いカード側では、ステップB4にて、上記ターミナル側にて入力された暗証番号PINを受信し、ステップB5にてその受信暗証番号をPINメモリ29記憶させる。これにより、暗証番号PINは、カード所有者以外の何人にも知られず、ICカード8内に登録されるようになり、その使用が可能となる。この後、同様にして、他の種類の複数のICカードにPINの設定登録を行なうと、その都度ターミナル1側の暗証情報メモリ12には、各カード固有のデータX₂、X₃、…及びこのカード固有のデータに対応するメモリ位置に、順次暗証番号PIN2、PIN3、…が順次書込まれるようになる。

一方、上記ステップB2においてN(No)、つまりカード側に予め登録されている照合番号(IPIN)とターミナル側より入力した照合番号I PINとが一致しない場合には、ステップB6に進み、カード側のシステム制御部25はター

ミナル側に対してBADメッセージを送信する。すると、ターミナル側では、上記ステップA5においてN(No)と判定され、エラー判断が下されるようになる。この場合、上記ステップA2におけるキー入力ミス、あるいはICカード8そのものがこのターミナルに対応していないと判断され、再びステップA1あるいはA2からの操作を行なう。

次に、上記第4図および第5図における暗証番号PIN設定後のICカード8使用中に、例えばカード所有者自身が自分の暗証番号PINを忘れてしまった場合におけるPINの読み出し動作を、第6図および第7図に示すフローチャートを参照して説明する。

第6図はターミナル付プリンタ電卓1内のフローチャートを、第7図はICカード8内のフローチャートを示すもので、まず始めに、ステップC1において、ターミナル付プリンタ電卓1のカード挿入口7に対して暗証番号PINを忘れたICカード8の一端を挿入し、そのそれぞれの接続端

子20、21の電気的接続を図る。すると、ICカード8では、ステップD1に示すように、システムROM24に記憶されたプログラムに従ってICカード特定化データメモリ27よりこのカード固有のデータXが取出され、カードを特定化するためのデータとして送信される。するとターミナル側では、ステップC2に示すように、上記カード側からの特定化データを受信し、ステップC3に進む。このステップC3では、上記カード側からの特定化データXに基づき、対応する暗証情報メモリ12内の固有のデータX₁を検索し、そのメモリ位置に記憶された暗証番号PIN1をこのICカード8に対応するものとして認識し特定化する。この後、ステップC4に進み、上記ステップC3にて特定化した暗証番号PIN1を暗証情報メモリ12より取出しICカード8に送信する。すると、カード側ではステップD2に示すように、上記ターミナル側から送られた暗証番号PINを受信し、暗証情報保持用RAM30にて一時記憶保持する。そしてステップD3に進み、上

記受信後にRAM30にて保持されたPINと、すでにPINメモリ29内に設定登録されている(PIN)とを比較部31にて比較照合する。このステップD3においてY(Yes)、つまり上記互いの暗証番号は一致[PIN=(PIN)]するものであり、このカード8は確かに現在接続中のターミナル付プリンタ電卓1に対応するものであると判定されると、システム制御部25は、ステップD4においてOKメッセージを送信する。すると、ターミナル側では、ステップC5にて、上記カード側からのメッセージ信号を受信し、ステップC6にて、そのメッセージ信号はOKメッセージであるか否かを判定する。このステップC6においてY(Yes)、つまり上記カード側からのメッセージ信号がOK信号であり、現在接続中のICカード8は、確かにこのターミナル1によってPINを設定登録したものであると判定されると、ステップC7に進み、上記ステップC3にて特定化した暗証番号PIN1を、システム制御部16の指定により暗証情報メモリ12より取

出し、表示制御部17を介して表示部3に表示させる。この場合、表示部3にて表示されるICカード8のPIN1は、比較的短時間の間(例えば5秒間)のみ表示されて消滅するもので、これによりカード所有者は、全く他人に知られることなく自分のICカード8のPINを知る事ができ、再びこのカードの通常通りの使用が可能となる。

この後、ステップC8に進み、システム制御部16および演算制御部14により、現在切換スイッチ9がその切換位置1、2、3の何れの位置に設定されているかを判断し、スイッチ位置1と判断された場合にはステップC9に進む。このステップC9では、上記ステップC7にてすでに表示した暗証番号PIN1以外のその他のPINデータ(この場合PIN2、PIN3、...)を、ステップD5に示すようにカード側より取出し、表示部3にて表示を行なうもので、これにより、例えばカード所有者が上記ICカード8以外のカード暗証番号をも忘れてしまっているとしても、直ちに確認することが可能である。また、上記ステッ

プC8において、スイッチ位置2と判断された場合には、ステップC10に進み、ターミナル1はICカード8における通帳メモリ28内の残高データを、上記と同様にしてステップD5において取出し表示部3に表示させる。これにより、カード所有者は、忘れたPINだけでなく、通帳残高までも確認することができる。さらに、上記ステップC8において、スイッチ位置3と判断された場合には、上記ステップC9およびC10で表示したようなカード内の諸データを上記カード側よりステップD5において取出し、印字制御部18を介して印字部4にて順次印字させる。これにより、上記通帳データなどを印字して確認することも可能である。

一方、上記カード側のステップD3においてN(No)、つまりステップC4にてターミナル側より送られたPINが、カード内にすでに設定登録された(PIN)とは一致せず、このICカード8は上記のターミナル付プリンタ電卓1に対応するものではないと判定されると、ステップD6

に進み、カード側のシステム制御部24は上記ターミナル側に対してBADメッセージを送信する。するとターミナル1側のステップC6においてはN(No)、つまり上記ICカード8はこのターミナル1によってPINを登録したものではないカードであると判定され、暗証情報確認のフローチャートはエラー判断状態となる。この場合、ICカード8はどこかで盗難されたものである可能性が非常に高く、ターミナル内の暗証情報あるいはその他の通帳データ等の諸データは、全く表示あるいは印字もされないままの状態となる。これにより、カードの不正所有者には、絶対にそのカード内容を知られることはない。

したがって、真のカード所有者が自分自身の暗証番号PINを忘れてしまった場合でも、全く他人に知られることなく再び自分のPINを確認することが可能となる。この場合、例えば盗難されたICカードについては、そのカードに対応するターミナルをも一緒に盗難されない限り、カード内容を知られることはなく、不正使用は未然に防

止されるようになる。

尚、上記実施例におけるターミナル付プリンタ電卓1は、カード所有者による本人管理でも、あるいはカード発行会社等による一括管理の何れでもよいが、後者カード発行会社等による管理の場合には、カード所有者は、上述したようなPIN設定あるいはPINの確認を、上記カード会社に出向いて行なうことになる。この場合、当然本ターミナル1は、カード会社の窓口設置される。

また、上記実施例におけるターミナル1は、前記第1図にも示されるように、通常はプリンタ電卓として使用可能であることは言うまでもない。

【発明の効果】

以上のようにこの発明によれば、ICカードに対する暗証情報の書込みと同時に予め本装置にもその暗証情報を記憶させておき、後に接続されるICカードからの固有信号によりそのカードの種類を認識し、この認識された特定ICカードに対応する上記予め記憶させた暗証情報と上記特定ICカード自身の記憶する暗証情報とを比較照合し、

この照合される互いの暗証情報が一致した際にその暗証情報を出力確認できるように構成したので、例えばカード所有者本人が自分の暗証番号を忘れてしまった場合には、カード内部に記憶された暗証情報を再び確認することができ、しかもカードの不正所有者に対してはそのカード内容を知ることが極めて困難であるICカード用暗証情報確認装置を提供できる。

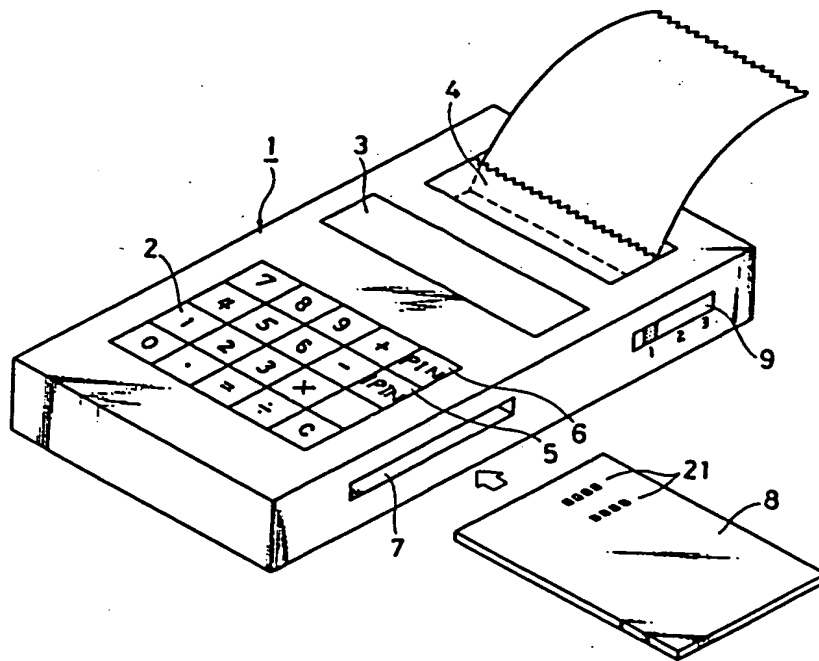
4. 図面の簡単な説明

第1図はこの発明の一実施例に係わるICカード用暗証情報確認装置を示す外観構成図、第2図は上記ICカード用暗証情報確認装置におけるターミナル付プリンタ電卓の回路構成図、第3図は上記ICカード用暗証情報確認装置におけるICカードを示す回路構成図、第4図および第5図はそれぞれ上記ICカード用暗証情報確認装置による暗証番号PIN設定の際のターミナル側およびカード側の動作を示すフローチャート、第6図および第7図はそれぞれ上記ICカード用暗証情報確認装置による暗証番号PIN確認の際のターミ

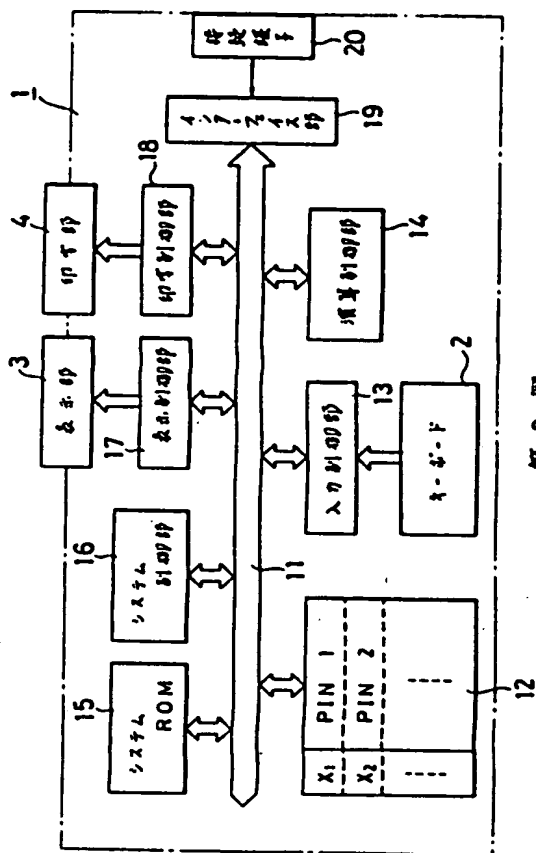
ナル側およびカード側の動作を示すフローチャートである。

1…ターミナル付プリンタ電卓、2…キーボード、3…表示部、6…PINキー、7…カード挿入口、8…ICカード、11、23…バスライン、12…暗証情報メモリ、19、22…インターフェイス部、20、21…接続端子、27…ICカード特定化データメモリ、29…PINメモリ、30…暗証情報保持用RAM、31…比較部。

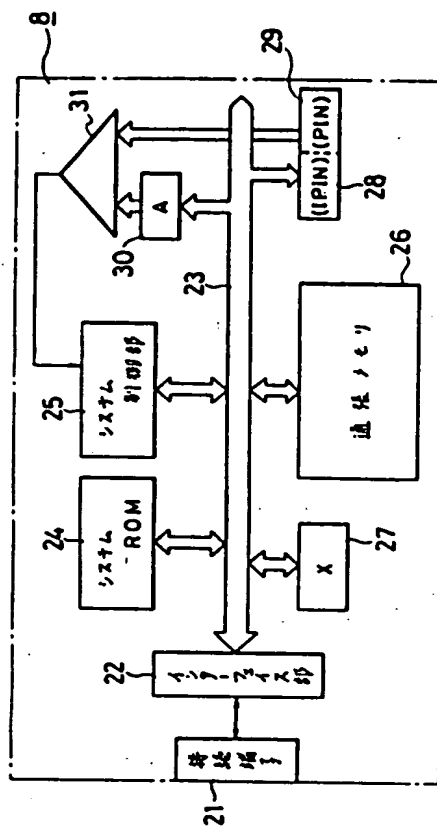
出願人 カシオ計算機株式会社



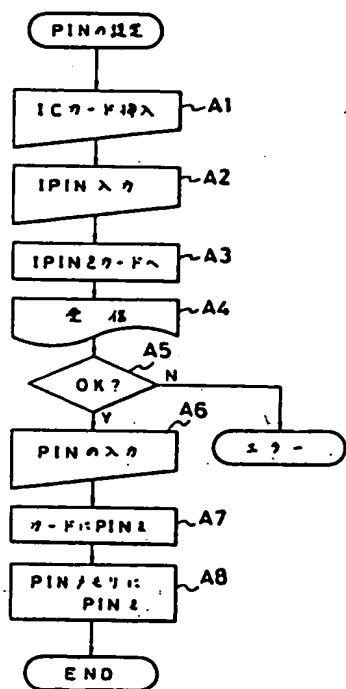
第1図



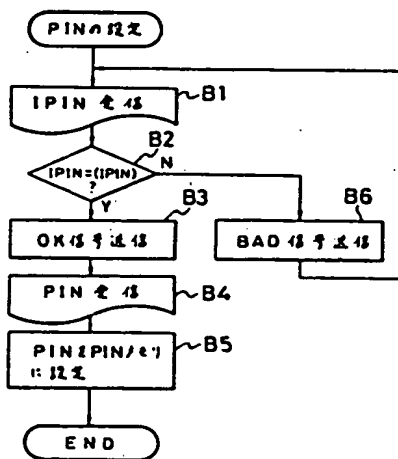
第2図



第3図



第4図



第5図

